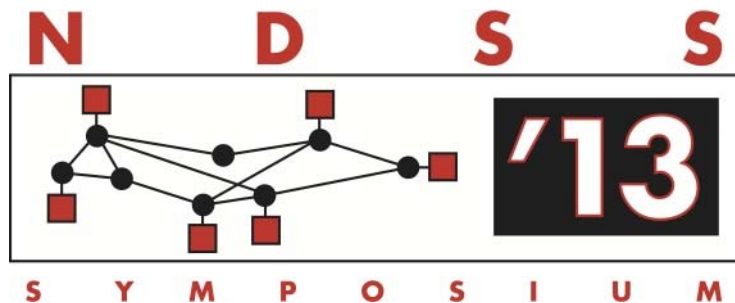Proceedings

2013

Network and Distributed System Security Symposium

Proceedings

2013

Network and Distributed System Security Symposium

February 24 – 27, 2013

San Diego, California

Sponsored by the
Internet Society

Internet Society
1775 Wiehle Avenue
Suite 201
Reston, VA 20190-5108

ISBN Number (Digital Format) 1-891562-34-7

Additional copies may be ordered from:

Internet Society
1775 Wiehle Avenue
Suite 201
Reston, VA 20190-5108
tel +1 703.439.2120
fax +1 703.326.9881
http://www.internetsociety.org

Table of Contents

Attack Surface Metrics and Automated Compile-Time OS Kernel Tailoring
   A. Kurmus, R. Tartler, D. Dorneanu, B. Heinloth, V. Rothberg, A. Ruprecht,
   W. Schröder-Preikschat, D. Lohmann, R. Kapitza

Taming Hosted Hypervisors with (Mostly) Deprivileged Execution
   C. Wu, Z. Wang, X. Jiang

When Firmware Modifications Attack: A Case Study of Embedded Expectation
   A. Cui, M. Costello, S.J. Stolfo

CAMP: Content-Agnostic Malware Protection
   M.A. Rajab, L. Ballard, N. Lutz, P. Mavrommatis, N. Provos

SESSION 4: Web Security

InteGuard: Toward Automatic Protection of Third-Party Web Service Integrations
   L. Xing, Y. Chen, X.F. Wang, S. Chen

Preventing Side-Channel Leaks in Web Traffic: A Formal Approach
   M. Backes, G. Doychev, B. Köpf

NeighborWatcher: A Content-Agnostic Comment Spam Inference System
   J. Zhang, G. Gu

AuthScan: Automatic Extraction of Web Authentication Protocols From Implementations
   G. Bai, J. Lei, G. Meng, S.S. Venkatraman, P. Saxena, J. Sun, Y. Liu, J.S. Dong

The Postman Always Rings Twice: Attacking and Defending postMessage in HTML5
   Websites
   S. Son, V. Shmatikov

SESSION 5: Social Networks and Application Security

Pisces: Anonymous Communication Using Social Networks
   P. Mittal, M. Wright, N, Borisov

Preserving Link Privacy in Social Network Based Systems
   P. Mittal, C. Papamanthou, D. Song

COMPA: Detecting Compromised Accounts on Social Networks
   M. Egele, G. Stringhini, C. Kruegel, G. Vigna

SESSION 6: Mobile and Wireless Security and Privacy

Social Turing Tests: Crowdsourcing Sybil Detection
   G. Wang, M. Mohanlal, C. Wilson, X. Wang, M. Metzger, H. Zheng, B.Y. Zhao

Comparing Mobile Privacy Protection through Cross-Platform Applications
   J. Han, Q. Yan, D. Gao, J. Zhou, R. Deng

On Implementing Deniable Storage Encryption for Mobile Devices
A. Skillen, M. Mannan

Contextual Policy Enforcement in Android Applications with Permission Event Graphs
*K.Z. Chen, N. Johnson, V. D'Silva, S. Dai, K. MacNamara, T. Magrino, E. Wu,
M. Rinard, D. Song*

Low-cost Standard Signatures in Wireless Sensor Networks: A Case for Reviving
Pre-computation Techniques?
G. Ateniese, G. Bianchi, A. Capossele, C. Petrioli

SESSION 7: Network Security I

Clickonomics: Determining the Effect of Anti-Piracy Measures for One-Click Hosting
T. Lauinger, M. Szydlowski, K. Onarlioglu, G. Wondracek, E. Kirda, C. Kruegel

FRESCO: Modular Composable Security Services for Software-Defined Networks
S. Shin, P. Porras, V. Yegneswaran, M. Fong, G. Gu, M. Tyson

Intention and Origination: An Inside Look at Large-Scale Bot Queries
J. Zhang, Y. Xie, F. Yu, D. Soukal, W. Lee

Juice: A Longitudinal Study of an SEO Botnet
D.Y.Wang, S.Savage, G.M. Voelker

I want my voice to be heard: IP over Voice-over-IP for unobservable censorship
circumvention
A. Houmansadr, T. Riedl, N. Borisov, A. Singer

SESSION 8: Short Talks

SESSION 9: Privacy and Anonymity

One (Block) Size Fits All: PIR and SPIR with Variable-Length Records via Multi-Block
Queries
R. Henry, Y. Huang, I. Goldberg

rBridge: User Reputation based Tor Bridge Distribution with Privacy Preservation
Q. Wang, Z. Lin, N. Borisov, N.J. Hopper

An Empirical Evaluation of Relay Selection in Tor
C. Wacek, H. Tan, K. Bauer, M. Sherr

SESSION 10: Anonymity, Authentication and Attacks

LIRA: Llightweight Incentivized Routing for Anonymity
R. Jansen, A. Johnson, P. Syverson

KinWrite: Handwriting-Based Authentication Using Kinect
J. Tian, C.Qu, W. Xu, S. Wang

Tailing RFID Tags for Clone Detection
D. Zanetti, S. Capkun, A. Juels

One Bad Apple: Backwards Compatibility Attacks on State-of-the-Art Cryptography
T. Jager, K.G. Paterson, J. Somorovsky

Does Counting Still Count? Revisiting the Security of Counting based User Authentication
Protocols against Statistical Attacks
H.J. Asghar, S. Li, R. Steinfeld, J. Pieprzyk

SESSION 11: Distributed Systems Security

Toward Online Verification of Client Behavior in Distributed Applications
R.A. Cochran, M.K. Reiter

Clear and Present Data: Opaque Traffic and its Security Implications for the Future
A.M. White, S. Krishnan, M. Bailey, F. Monrose, P. Porras

Verito: A Practical System for Transparency and Accountability in Virtual Economies
R. Bhaskar, S. Guha, S. Laxman, P. Naldurg

Secure Computation on Floating Point Numbers
M. Aliasgari, M. Blanton, Y. Zhang, A. Steele

Analyzing Unique-Bid Auction Sites for Fun and Profit
O. Samorodnitzky, E. Tromer, A. Wool

SESSION 12: Network Security II

Fix Me Up: Repairing Access-Control Bugs in Web Applications
S. Son, K.S. McKinley, V. Shmatikov

Automatically Inferring the Evolution of Malicious Activity on the Internet
S. Venkataraman, D. Brumley, S.Sen, O. Spatscheck

Detection of Malicious PDF Files Based on Hierarchical Document Structure
N. Šrndič, P. Laskov

Behind the Scenes of Online Attacks: an Analysis of Exploitation Behaviors on the Web
D. Canali, D. Balzarotti

General Chair's Message

It is my pleasure to welcome you all back to the beautiful Catamaran Resort Hotel and Spa on Mission Bay in San Diego for the Internet Society's Network and Distributed System Security Symposium (NDSS'13). This year's meeting is a milestone for us and we thank you for helping us celebrate the Twentieth Anniversary of what started out as the "PSRG Workshop on Network and Distributed System Security." That informal two-day workshop, held right here at the Catamaran on February 11-12, 1993, was such a unique and successful event that we are now in our 20th year. We still offer a unique and highly intellectual symposium. Many thanks to the original workshop chairman, Dan Nessett, then of Lawrence Livermore National Labs, along with the 1992 PSRG, for creating such a high quality and successful symposium, one that I hope continues another 20 years and more. I wish to especially recognize NDSS' previous chairs: Dan Nessett (1993-94), James Ellis (1995-96), David Balenson (1997-98), Steve Welke (1999-01), Cliff Neuman (2002-04), Eric Harder (2005-07), and Doug Szajda (2008-11).

I would like to thank the Catamaran Resort for providing such an excellent venue. Even though we have switched venues several times over the last twenty years, I'm not sure we would be here today without the help of the fantastic staff of this facility. Their willingness to allow a no-name, informal group of security and network researchers to reserve their meeting and hotel rooms back in 1993 with virtually no collateral or history is what allowed this symposium to be born.

From our very first workshop and continuing today, NDSS has striven to maintain the superior quality of our technical program. Our research domain continues to emphasize practical applications of security based on solid theoretical foundations. The program stretches from canonical to current, and includes both the theoretical and the pressing need. This scope, along with a willingness to consider potentially controversial or unusual research, is the essential beauty of NDSS.

The program for this year packs a lot into three days and includes twelve sessions and forty-seven original research papers. They cover a variety of current topics such as the security and privacy of mobile devices, cloud computing, distributed systems and networks, web security and privacy, intrusion detection and attack analysis, anonymity, and more. Our three keynote speakers are: Dr. Richard Kemmerer, Computer Science Leadership Chair at University of California Santa Barbara; Stephen Smalley of the Trusted Systems Research Group at the US National Security Agency (NSA); and Joe Sullivan, Chief Security Officer of Facebook. The Program Committee has also included twelve short talks.

Although the symposium revolves around the technical presentations, there is far more to the experience. You are encouraged to take advantage of the hall track, the lunches, and the dinners to meet new colleagues. Participate in discussions, always an invaluable part of disseminating information. Remember also to take in our fantastic geographic location.

This symposium is possible only through the hard work of many people. The Steering Group, which I am pleased to co-chair with Lynn St. Amour from the Internet Society, expertly charts a course for the conference that keeps its focus current, relevant, and practical. Andrew M. White skillfully assembled the *Proceedings* as Publications Chair. Kevin Craemer has done a wonderful job of finding sponsors and helping plan and publicize the conference and Terry Weigler, as always has done a fantastic job dealing with each and every one of you for Registration.

This meeting is as enjoyable and as successful as it is because of the efforts of these people -- it is no exaggeration to say that NDSS simply would not happen without each of their contributions.

The quality of this conference directly depends upon the quality of the papers and short talks accepted. The Program Committee, under the direction of Program Chair Peng Ning of North Carolina State University and Samsung Mobile, has done a fantastic job and selected an extraordinary set of papers. I thank Peng and the entire Program Committee for their expertise, hard work, and dedication. I also thank the authors who submitted papers and the speakers who are present; YOU are the core of this symposium.

I want to thank our sponsors, as it would be impossible to hold such an event without them. Our sponsors are the Internet Society for overall sponsorship, Internet2 for Gold Sponsorship; Afilias, FishNet Security, Qualcomm, and the San Diego Supercomputer Center @ UCSD (SDSC) for Silver sponsorship; Research at Google and Microsoft Research for Bronze sponsorships, and IEEE Security and Privacy Magazine as our media sponsor. The conference is organized by the Internet Society, in cooperation with USENIX.

I would also like to thank my organization, the San Diego Supercomputer Center at the University of California San Diego, for supporting my involvement with this symposium for the last twenty years. Finally, I want all of you to know that I consider it a great honor to chair this conference, one where the attendees and speakers are some of the finest minds in computer security.

<div align="center">

Thomas Hutton,
NDSS'13 General Chair
San Diego Supercomputer Center
University of California San Diego
hutton@sdsc.edu

</div>

Program Chair's Message

It is my great pleasure to welcome you to the 20th Annual Network & Distributed System Security Symposium (NDSS 2013) held in Catamaran Resort Hotel and Spa, San Diego, CA, United States, February 24-27, 2013. NDSS fosters information exchange among researchers and practitioners of network and distributed system security. The target audience includes those interested in practical aspects of network and distributed system security, with a focus on actual system design and implementation. A major goal is to encourage and enable the Internet community to apply, deploy, and advance the state of network and distributed systems security technologies.

This year NDSS received 250 valid submissions (after removing papers that clearly violated the submission guidelines). These papers were evaluated on the basis of their significance, novelty, and technical quality. All these papers went through two rounds of reviews, evaluated by at least three members of the Program Committee (PC) with a few exceptions. The discussion among the PC members was first held online for a period of two weeks, followed by 1.5 days face-to-face PC meeting. Finally, among the 250 submissions, 47 papers were selected to be published in the conference proceedings. This gives an acceptance ratio of 18.8%.

The NDSS 2013 program will also feature 3 keynote speakers. In recognition of the 20th anniversary of NDSS, Richard Kemmerer of UC Santa Barbara will kick off on the first day of conference with a 20-year review of network and distributed systems security. On the second day of the conference, Stephen Smalley of the National Security Agency will lay out a vision for secure mobile computing, including a discussion of the roles that virtualization, trusted computing, and secure operating systems play in an overall security architecture and how these mechanisms can be realized in mobile devices today. On the third day of the conference, Joe Sullivan of Facebook will give examples of several different ways his team has evolved dramatically in the last years to address the growing security challenges faced by Facebook's unprecedented development around the world.

This year NDSS will try something new. The PC invited another 12 papers to be presented as short talks at the conference. These are the submissions that the Program Committee considered to have fresh and exciting ideas, though they couldn't be accepted as regular papers. We expect these short talks will bring more excitement to NDSS 2013.

There is a long list of people who volunteered their time and energy to put together the symposium and who deserve acknowledgment. Our special thanks go to Kevin Craemer, who handled all the logistics of NDSS 2013. It would be impossible to have NDSS 2013 without his continuous hard work. I would also like to thank Lujo Bauer, who served as the Shadow PC Chair to handle the submissions that have conflict with the PC Chair. Lujo's support during the PC meeting was also indispensable. I am grateful to Andrew White for serving as the Publication Chair for NDSS 2013, and to the student volunteer Wenbo Shen, who spent 1.5 days with the Program Committee to provide the logistic supports during the PC meeting. Special thanks to the PC members and external reviewers for all their hard work during the review and the paper selection process. I would like to thank the General Chair of NDSS 2013, Tom Hutton for the leadership at the conference. Last, but certainly not least, our thanks go to all the authors who submitted papers and all the attendees. We hope that you will find the program stimulating and a source of inspiration for future research.

Peng Ning
Program Chair, NDSS'13
North Carolina State University and Samsung Mobile

Program Committee Members

Peng Ning (Chair), NC State University and Samsung Mobile

Ehab Al-Shaer, UNC Charlotte,
Yair Amir, Johns Hopkins University
Michael Backes, Saarland University and MPI-SWS, Germany
Dirk Balfanz, Google
Davide Balzarotti, EURECOM, France
Lujo Bauer, Carnegie Mellon University
Steven Bellovin, Columbia University
Elie Bursztein, Google
Srdjan Capkun, ETH Zurich, Switzerland
Marc Dacier, Symantec, France
Wenliang Du, Syracuse University
William Enck, NC State University
Úlfar Erlingsson, Google
Nick Hopper, University of Minnesota
Xuxian Jiang, NC State University
Apu Kapadia, Indiana University
Stefan Katzenbeisser, TU Darmstadt, Germany
Roger Khazan, MIT Lincoln Lab
Yongdae Kim, University of Minnesota and KAIST, South Korea
Engin Kirda, Northeastern University
Jun Li, University of Oregon
Ninghui Li, Purdue University
Zhichun Li, NEC Laboratories America
Zhenkai Liang, National University of Singapore, Singapore
Yao Liu, University of South Florida
Jonathan McCune, Carnegie Mellon University
Patrick McDaniel, Penn State University
John Mitchell, Stanford University
David Molnar, Microsoft Research
Cristina Nita-Rotaru, Purdue University

Alina Oprea, RSA Laboratories
Bryan Parno, Microsoft Research
Radha Poovendran, University of Washington
Phillip Porras, SRI International
Zhiyun Qian, NEC Laboratories America
Michael Reiter, UNC Chapel Hill
Kui Ren, Illinois Institute of Technology
Thomas Ristenpart, University of Wisconsin
Volker Roth, Freie Universität Berlin, Germany
Ahmad-Reza Sadeghi, TU Darmstadt, Germany
Pierangela Samarati, Università degli Studi di Milano, Italy
Elaine Shi, University of Maryland
Radu Sion, Stony Brook University
Robin Sommer, ICSI/LBNL
Abhinav Srivastava, AT&T Labs
Wade Trappe, Rutgers University
Patrick Traynor, Georgia Institute of Technology
David Wagner, UC Berkeley
Cliff Wang, Army Research Office
XiaoFeng Wang, Indiana University
Venkat Venkatakrishnan, University of Illinois at Chicago
Tao Wei, UC Berkeley, USA, and Peking University, China
Glenn Wurster, Research In Motion Limited, Canada
Yinglian Xie, Microsoft Research
Dongyan Xu, Purdue University
Heng Yin, Syracuse University
Moti Yung, Google
Xiaolan Zhang, IBM Research
Yanchao Zhang, Arizona State University

Conference Committee

General Chair
Thomas Hutton
San Diego Supercomputer Center @ UCSD
hutton@sdsc.edu

Program Chair
Peng Ning
North Carolina State University and Samsung Mobile
pning80@gmail.com

Publications Chair
Andrew White
University of North Carolina
amw@cs.unc.edu

Publicity Chair
Kevin Craemer
Internet Society
craemer@isoc.org

Local Arangements Chair
Thomas Hutton
San Diego Supercomputer Center @ UCSD
hutton@sdsc.edu

Conference Coordinator
Kevin Craemer
Internet Society
craemer@isoc.org

Sponsorship Coordinator
Kevin Craemer
Internet Society
craemer@isoc.org

NDSS Steering Group

Co-Chairs

Thomas Hutton
San Diego Supercomputer Center
University of California, San Diego

Lynn St.Amour
Internet Society

Administrative Coordinator

Kevin Craemer
Internet Society

Steering Group Members

Lujo Bauer
Carnegie Mellon University

Yongdae Kim
*Korea Advanced Institute of Science
and Technology*

Tadayoshi (Yoshi) Kohno
University of Washington

Wenke Lee
Georgia Institute of Technology

David Molnar
Microsoft Research

Peng Ning
*North Carolina State University &
Samsung Mobile*

Clifford Neuman
University of Southern California

Adrian Perrig
Carnegie Mellon University

Michael Roe
University of Hertfordshire

Doug Szajda
University of Richmond

Giovanni Vigna
University of California, Santa Barbara